Abstract

An encryption transmission apparatus and an encryption reception apparatus avoid attack that takes advantage of a re-transmission request. A server apparatus encrypts a content key five times, thereby generating five encrypted content keys, calculates a hash value of the content key, and transmits the five encrypted content keys and the hash value. An image playback apparatus receives the five encrypted content keys and the hash value, decrypts the five encrypted content keys thereby generating five content keys, calculates hash values, each corresponding to the generated content keys, and compares the calculated hash values with the received hash value, respectively. If at least one of the five calculated hash values matches the received hash value, the corresponding content key is considered correct. Conversely, if none of the five calculated hash values matches the received hash value, it is considered a decryption error.